REMARKS

Claims 1-8, 10-11, and 13-23 are pending in the application. Claims 1-2, 4, 6, 8, 10-11, 13, 15, 17, and 19-23 are amended herein. Claims 9 and 12 were previously canceled. Claims 3, 5, and 7 are canceled without prejudice herein. No claims have been allowed.

Rejections under 35 U.S.C. § 103

Claims 1-24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Jerger et al. (U.S. Patent No. 6,473,800), hereinafter "Jerger", in view of Starr (U.S. Patent No. 6,606,606 hereinafter "Starr").

Applicants respectfully submit that the claims are patentable over the cited art.

Jerger describes configuring a Windows operating system on a personal computer so that the personal computer is more secure when browsing the Internet. Jerger is directed toward providing security when downloading "foreign active content" from a computer network. Jerger describes "foreign active content" as untrusted code that may attempt to run on a host system. Jerger also discloses various security zones that correspond to a set of locations on a computer network. The architecture and method of Jerger involve a general purpose computer (as illustrated in Figure 1) and a browser (as illustrated in Figure 2). Jerger describes a method of making a general purpose computer more secure when the computer is in communication with a network. This is accomplished by the user of the general purpose computer performing various configuration steps according to Figure 3. Thus, Jerger is limited to configuring a general purpose computer to govern its behavior so as to secure against downloading certain foreign active content when browsing networks such as the Internet. Accordingly, once the general purpose computer is configured, it automatically behaves in an identical manner, no matter who the user may be, and the computer distinguishes between different downloadable content according to the configuration.

In contrast to Jerger, the claimed invention includes

> A method implemented by a financial analysis system, the method comprising:
>
> identifying multiple financial accounts associated with a user, wherein the multiple financial accounts are with a plurality of financial institutions;

presenting the user with a plurality of modes, each of which can be associated with one of the plurality of financial institutions, wherein the user has user authentication data for each of the plurality of financial institutions, and wherein each mode directs the financial analysis system to handle user authentication data received from the user in a specified manner, the modes comprising,

a low trust mode that directs the financial analysis system to temporarily use the user authentication data received from the user without storing the data; and

a plurality of higher trust modes that each direct the financial analysis system to store the user authentication data;

receiving a selection of a mode from the user for each of the multiple financial institutions;

associating a selected mode with each of the plurality of financial institutions;

storing financial institution data for each of the plurality of financial institutions, comprising data which may be used to locate and communicate with each of the plurality of financial institutions;

storing the associated modes; and

handling user authentication data associated with each of the plurality of financial institutions as directed by an associated mode each time the user accesses one of the multiple financial institutions.

(Claim 1 as amended).

Jerger does not disclose or suggest identifying multiple financial accounts associated with a user, wherein the multiple financial accounts are with a plurality of financial institutions. Jerger further fails to disclose or suggest presenting the user with a plurality of modes, each of which can be associated with one of the plurality of financial institutions, wherein the user has user authentication data for each of the plurality of financial institutions, and wherein each mode directs the financial analysis system to handle user authentication data received from the user in a specified manner. Jerger fails to teach that the user may select a mode or change a mode at any time.

Jerger lacks any teaching regarding user authentication data for financial institutions. Jerger is limited to setting up a personal computer to control what can be downloaded from a network to the computer. This is in contrast to claim 1, which includes modes that direct a financial analysis system to handle user authentication data received from the user in a specified manner, where the user authentication data is for one of a plurality of financial institutions. The financial institutions are entities other than any computer the user may be using. The teaching of Jerger is confined with setting up a

user computer and does not touch on receiving a selection of a mode that has an effect on how user authentication data for accessing another entity is handled.

Starr describes a middleware product hosted on a server and accessed by small businesses which use the middleware to centralize their online business interactions with banks and the like. The security features described in Starr are limited to attempting to assure that a subscriber does not perform a function that is not unauthorized for that particular user, such as issuing a company check, while in communication with a bank online.

Starr is directed toward a tool kit for a small business owner to manage a plurality of different financial accounts to perform a number of different financial transactions, wherein each of the transactions involves multiple sub-transactions which occur among different financial service providers. For example, the system provides an integrated package that integrates financial service providers, such as a payroll service provider, a retirement plan service provider, a healthcare service provider or another type of service provider. The system provides one interface to a subscriber and the subscriber can select from the interface a financial transaction to perform. (Column 2, lines 52).

> Figure 2 illustrates a system according to Starr in which:
>
> [a] subscriber 12 employs a user interface 32 to provide user input to the server 14. As can be seen from FIG. 2, the server 14 acts as middleware that coordinates the operations of the financial service providers 28 and 30 to allow perform a compound or integrated financial transaction, that involves the services of both these service providers. Specifically, the server 14 is as a functional block diagram that includes a web server 40, an access control module 42, an instruction generator 44 and a report generator 48.
> (Column 6, lines 58-67).

The access control module allows the system to be configured so that various subscribers have different levels of access to the server 14. The access controller can determine whether the company name, user name and password indicate that the subscriber has a valid account on the server 14. In optional embodiments, the access controller can determine the class of access to grant the subscriber. For example, in these optional embodiments, each account can have a root user that is capable of creating sub accounts on the server, each sub account having different levels of user privileges. For

example, the root user, or admin, can provide certain users with read only access to the company account information. Further, the root user may restrict a subaccount user to certain transactions. Thus, the payroll person for the company may be allowed to employ the payroll service, but may be prevented from accessing the CMA account for general check writing privileges. (Column 7, lines 18-33).

Thus, Starr describes a system including middleware accessed by subscribers, wherein the middleware can be configured to allow different access privileges to different subscribers. Starr does not disclose or suggest user-selectable modes that indicate how user authentication data will be handled. In contrast, Starr teaches configuring middleware to distinguish among different users with different levels of privilege to access a server. This is to be distinguished from the claimed modes, because Starr's levels of privilege have nothing to do with how user authentication data is handled by Starr's server. Starr does not disclose allowing to the user to select how user authentication data (that allows access to other entities such as financial institutions) will be handled for various institutions. Rather, Starr discloses allowing a user to limit what other users can do once the other users are logged onto an institution's site. Starr, in contrast to the claimed invention, always stores user authentication data in the server without giving the user a choice to avoid storing the data in the server. For example, at column 5, lines 58-63, Starr states:

> The server 14 may couple to a database 16 that stores information representative of a subscriber's account, including information about the different financial service providers that the subscriber employs and [stores] information regarding the subscribers accounts, including passwords, user accounts, user privileges and similar information.
> (column 5, lines 58-63, emphasis added)

Starr nowhere mentions a user-selectable mode that directs a system to temporarily use the user authentication data (such as passwords) received from the user without storing the data. Starr does not supply the deficiencies of Jerger because Starr, alone or in combination with Jerger, fails to teach or suggest presenting the user with a plurality of modes as claimed, or receiving a selection of a mode from the user. Starr does not disclose or suggest handling sensitive data associated with each of the plurality of financial institutions in accordance with an associated mode as claimed. The claimed

invention includes modes associated with financial institutions as selected by a user. The selected mode dictates the manner in which the financial analysis system handles the user's sensitive data, such as whether the data is stored and how it is stored. Applicants respectfully submit that the proposed combination fails to teach or suggest at least identifying, receiving, associating and handling as in claim 1.

Therefore, Applicants respectfully submit that claim 1 would not have been obvious in view of the prior art.

Applicants further submit that one of ordinary skill in the art would find no motivation to combine the references as suggested in order to arrive at the claimed invention. For example, Jerger describes configuring a Windows operating system on a personal computer so that the personal computer is more secure when browsing the Internet. Starr describes a middleware product hosted on a server and accessed by small businesses which use the middleware to centralize their online business interactions with banks and the like. The security features described in Starr are limited to attempting to assure that a subscriber does not perform a function that is not unauthorized for that particular user, such as issuing a company check, while in communication with a bank online There is no relationship between Jerger and Starr such that one of ordinary skill would be motivated to combine the two references to achieve the multiple mode method as claimed.

Claims 2, 4, 6, and 8 depend from claim 1 and include further limitations thereon. For this reason, Applicants respectfully submit that claims 2, 4, 6, and 8 are similarly allowable over the cited references.

Claim 10 recites a method including the limitations of claim 1 as distinguished from the cited art above. In addition, claim 10 further includes a low trust mode and a high trust mode. Applicants respectfully request that the remarks with reference to claim 1 be applied to claim 10 as well. Applicants respectfully submit that claims 10, 11, 13, and 14 are allowable over the cited references for at least the same reasons given with reference to claim 1.

Claim 15 recites a method including the limitations of claim 1 as distinguished from the cited art above. In addition, claim 15 further includes a moderate trust mode and a high trust mode. Applicants respectfully request that the remarks with reference to

claim 1 be applied to claim 15 as well. Applicants respectfully submit that claims 15 and 16 are allowable over the cited references for the same reasons given with reference to claim 1.

Claim 17 recites a method including the limitations of claim 1 as distinguished from the cited art above. In addition, claim 17 further includes a moderate trust mode and a low trust mode. Applicants respectfully request that the remarks with reference to claim 1 be applied to claim 17 as well. Applicants respectfully submit that claims 17 and 18 are allowable over the cited references for the same reasons given with reference to claim 1.

Claim 19 recites one or more computer-readable media including the limitations of claim 1 as distinguished from the cited art above. Applicants respectfully request that the remarks with reference to claim 1 be applied to claim 19 as well. Applicants respectfully submit that claims 19-23 are allowable over the cited references for the same reasons given with reference to claim 1.

CONCLUSION

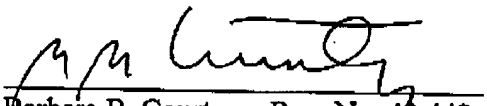
In view of the foregoing amendments and remarks, Applicants respectfully submit that claims 1-2, 4, 6, 8, 10-11, and 13-23 are in condition for allowance. The allowance of the claims is earnestly requested. The Examiner is invited to call the undersigned if there are any issues that remain to be resolved prior to allowance of the claims.

AUTHORIZATION TO CHARGE DEPOSIT ACCOUNT

Please charge deposit account 503616 for any fees due, and not paid herewith, in connection with this Office Action response.

Respectfully submitted,
Courtney Staniford & Gregory LLP

Date: December 5, 2006



Barbara B. Courtney, Reg. No. 42,442
Tel. 408-342-1902

Courtney Staniford & Gregory LLP
P.O. Box 9686
San Jose CA 95157